Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1642 10/17/14

~ FBI Encryption Warning ~ People Are Talking! ~ New "Resident Evil"!
~ Titanfall Expansions! ~ Yosemite Preparation! ~ Keep Poodle at Bay!
~ Wild West of Domains! ~ NSA Reviews Side Jobs! ~ How Whisper Tracks!

-* Gamergate: A Scandal Erupts! *-
-* Facebook Automates Against Hackers! *-
-* Snapsaved Hack Led to Snapchat Photo Leak! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"

Yes, the Ebola scare is real. Of course, I believe that the world should do its utmost to protect its population from this dreadful disease. But, what really irks me is the stupidity some in the healthcare field is dealing with this. And, the CDC is even worse!

Why are hospital workers who have been involved in the treatment of Ebola patients allowed to travel? Why aren't these healthcare professionals going through some sort of post-care "quarantine" to determine their condition? Whatever happened to "Universal Precautions" procedures - something that should be even more enforced under these circumstances?

Has training lapsed over the years that these so-called professionals don't have an ounce of common sense? Sorry, I don't mean to put down the entire healthcare profession, but these events in Texas are beyond what should be expected. And I don't believe that something like this is limited to that Dallas hospital! I've heard on the news that nurses are trying to publicly express their lack of preparedness for something like this. That's scary!

Until next time...

=~=~=~=

->In This Week's Gaming Section - Resident Evil: Revelations 2!
Gamergate: A Scandal Erupts!
Titanfall Expansions!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

Resident Evil: Revelations 2 PlayStation Preorders Get Bonus Mode

According to Polygon, the game’s producer Michiteru Okabe revealed the news during a panel at the New York City Comic-Con. Preordering the game on PlayStation consoles will get you the Raid Mode Throwback, a variation of the Raid Mode introduced in the first game, which asks one or two players to fight their way through maps from the single player campaign populated with different enemies. Raid Mode Throwback will work the same, only with stages from previous Resident Evil games.

The game should be available to preorder on PS4 on October 14, and PS3 preorders should be available later this month.

Resident Evil: Revelations 2 will release in four episodes. You’ll be able to buy each for $6, or purchase all of them for $25. The $25 bundle includes the four chapters and some "additional game content," which will be announced later. Once the four episodes are released, Capcom will launch a disc-based version of Revelations 2, featuring the four chapters and additional content, for $40.

The game is coming to Xbox 360, Xbox One, PS3, PS4, and PC. As was previously rumored, it follows Claire Redfield and Barry Burton’s daughter, Moira Burton.

Xbox 360 Titanfall Players Get "IMC Rising" DLC Next Week

Respawn Entertainment has announced that Titanfall’s third DLC expansion, IMC Rising, will launch for Xbox 360 on October 21. The DLC was released for Xbox One and PC in September.

IMC Rising, which was announced at Gamescom in August, features three maps - Backwater, Zone 18, and Sandtrap. It follows previously released expansions Frontier’s Edge and Expedition. IMC Rising is the third expansion included with the $25 Titanfall DLC pass.

Gamers who don’t own the pass can buy IMC Rising (or the other two expansions) for $10 each. However, if you know for sure you want all three, the season pass will save you $5.

In addition to paid expansions, Respawn continues to support Titanfall with free stability/general improvement updates, while all non-map updates are also free.

Now that all scheduled Titanfall DLC has been released, the studio is likely moving its resources onto other projects, such as Titanfall 2, which was greenlit back in March, according to our sources. The game has not been officially announced, though publisher Electronic Arts confirmed in May that Respawn is indeed working on more "Titanfall experiences."

Gamergate: A Scandal Erupts in the Video-Game Community

Anita Sarkeesian s criticism of misogyny in video games has made her the target of violent threats.

At this year s Game Developers Choice Awards, the closest the video-game industry has to an Oscars ceremony, Anita Sarkeesian received the Ambassador Award, a prize that honors individuals who help the industry advance to a better place through advocacy or action. Sarkeesian, a Canadian-American feminist and media critic, won the award for creating a series of videos titled Tropes vs. Women in Video Games, which discuss and challenge sexism and misogyny in gaming. My project was born out of a desire to take gaming seriously, she said in her acceptance speech, adding that game developers can portray women as capable, complex, and inspirational.

Earlier, the award ceremony s organizers had received an anonymous e-mail that stated, A bomb will be detonated at the Game Developers Choice award ceremony tonight unless Anita Sarkeesian s Ambassador Award is revoked. We estimate the bomb will kill at least a dozen people and injure dozens more. It would be in your best interest to accept our simple request. This is not a joke. You have been warned. The message was just one example of the many threats that Sarkeesian had received since launching her video series. In 2012, the Times reported that Sarkeesian had been sent images showing video-game characters raping her. Her Wikipedia entry was repeatedly vandalized. One man created a Web game called Beat Up Anita Sarkeesian, in which players could punch Sarkeesian s image and watch her face become bruised. The violent threats have continued unabated; Sarkeesian fled her home in August after a Twitter user posted her address and threatened to kill her.

The most recent incident occurred on Tuesday, when the director of Utah State University s Center for Women and Gender received an e-mail proposing the deadliest school shooting in American history if Sarkeesian s upcoming speaking engagement at the school was not cancelled. The e-mail, which was published online by the Standard-Examiner, read, I have at my disposal a semi-automatic rifle, multiple pistols, and a collection of pipe bombs . Anita Sarkeesian is everything wrong with the feminist woman, and she is going to die screaming like the craven little whore that she is if you let her come to USU. Sarkeesian cancelled her talk after the campus police, citing Utah s gun laws, refused to prohibit attendees from carrying concealed weapons to the event. The e-mail is being considered as part of an ongoing F.B.I. investigation into threats against Sarkeesian.

These death threats are clearly the work of troubled minds. More mundane and more prevalent are the tens of thousands of messages that Sarkeesian has received that attempt to debunk her work and force her to silence. Speaking to Mother Jones in May, Sarkeesian said, The gaming industry has been male-dominated ever since its inception, but over the last several years there has been an increase in women s voices challenging the sexist status quo. We are witnessing a very slow and painful cultural shift. Some male gamers with a deep sense of entitlement are terrified of change.

Video games have, in recent years, begun to expand beyond the traditional themes of sports, racing, and warfare. The Cat and the Coup, for example, allows players to experience the life of the pet cat of Dr. Mohammad Mossadegh, the first democratically elected Prime Minister of Iran. Coolest Girl in School challenges its players to get through the day with a period stain on their skirts. This new subject matter has allowed critics, who have traditionally judged video games based on their

entertainment value, to broaden the lenses through which they approach a work.

But there are those who wish to close down these new lines of conversation and creativity, whether by campaigning for the removal of a relatively obscure piece of interactive fiction about depression, or by silencing critics like Sarkeesian who critique games through a feminist lens. Now the fear of change that Sarkeesian has identified (which is ultimately a fear that one s power or position will be compromised) has coalesced into a movement of sorts. Some of its participants have clustered around the banner #gamergate, a cringe-inducing Twitter hashtag popularized by the actor Adam Baldwin. Baldwin, seeking to point out an example of unethical journalism, linked on Twitter to a video claiming that a video-game writer had promoted work by the independent game-maker Zoe Quinn while the two were in a relationship. (This claim that has since been proved false.)

The Gamergate hashtag has been used more than a million times on Twitter, for myriad purposes. Some denounce harassment but consider the tag a demand for better ethical practices in video-game journalism, including more objective reporting and a removal of politics from criticism. (Never mind that Gamergate itself is awash in politics). Critics see Gamergate as a hate movement, born of extremists, which has grown by providing a sense of belonging, self-worth, and direction to those experiencing crisis or disaffection.

The Gamergate movement is tiny relative to the mainstream audience for games, and its collective aims are ambiguous, but it has still managed to make itself heard. After the Web site Gamasutra came under criticism for its connection to the hashtag, Intel removed advertising from the site. (Intel later claimed that it was unaware of the hashtag when it made its decision, but Gamasutra maintains that this is untrue. Intel ultimately apologized for pulling its ads.) Outside of Twitter, the tag s users continue to organize e-mail campaigns aimed at companies who advertise on gaming Web sites with whom they collectively disagree. Regardless of the aims and beliefs of any one individual using the tag, Gamergate is an expression of a narrative that certain video-game fans have chosen to believe: that the types of games they enjoy may change or disappear in the face of progressive criticism and commentary, and that the writers and journalists who cover the industry coördinate their message and skew it to push an agenda. It is a movement rooted in distrust and fear.

For those who have found refuge and sanctuary in video games (in virtual worlds that are ruled through fairness and justice, in which everyone can succeed if they follow the rules), the fear is that criticism is the first step toward censorship. They worry that the games that have been meaningful to them will change. Some feel that Sarkeesian, in criticizing games for their misogynistic portrayals of women, is also accusing those who enjoy the games of misogyny. Some believe that they are at risk of becoming an oppressed minority.

Criticism of video games used to come primarily from those who saw them as a shameful, wasteful pursuit that, at its worst, encouraged acts of violence among vulnerable young people. That argument (which has also been aimed at theatre and film) has largely passed. This time, it s the progressive voices from within the critics and creators who have given their professional lives over to the video games not out of hatred or suspicion but because they believe in the medium who must be driven out of town.

I have first-hand experience of this mentality. When I wrote about Zoe Quinn s game Depression Quest for this site last month, a piece that was commissioned before the coining of the Gamergate hashtag, my editor received a slew of messages from people who disagreed with the article and sought to discredit me by claiming that I had a financial connection to the story. I sponsor several writers with small monthly donations via Patreon, a crowdfunding Web site for artists. Unbeknownst to me, one of those writers, Jenn Frank, had been commissioned to write a piece for the Guardian about the harassment that Quinn had endured. This was enough for many Gamergate supporters to denounce my piece as part of a media conspiracy. I can t imagine how much worse it must be to receive threats against one s life.

Video games, like all art and entertainment, are inherently political; they are created worlds that can t help but express the values of their creators. Sometimes, those values are reflected in the demographics of the games: in how they represent, or fail to represent, women and minorities, or in the virtual foes they ask players to kill with their virtual guns. Other times, the systems and rules that govern games reflect and reinforce those that we experience on this side of the screen. The political nature of games is not something to fear, or to shy away from discussing. It is in part what makes them so fascinating. Strong criticism is neither an act of betrayal toward a work nor the first step toward censorship; it leads to illumination and improvement.

Those who wish to censor or expel certain creators and critics are often avid fans of video games, but their views are antithetical to its virtues. At their best, video games promote empathy and understanding by allowing us to experience virtual life from another s perspective. Those who stand against honest debate and dialogue may think that they are protecting a beloved pastime, but their actions compromise its vibrant future.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Confirmed: Snapsaved Hack Led to Snapchat Photo Leak

After word spread last week that some 200,000 Snapchat photos had leaked online, third-party site Snapsaved.com is now taking responsibility for the whole debacle.

In a Facebook post over the weekend, Snapsaved.com admitted that a recent hack of its systems led to the leak, and provided more clarity about the extent of the breach.

"I would like to inform the public that Snapsaved.com was hacked," the post reads. "Snapchat has not been hacked, and these images do not originate from their database."

The site’s creators said they "immediately" deleted their entire database upon discovering the breach. Some 500MB of images were stolen, and the majority of affected users are Swedish, Norwegian, and American. No other personal information was accessed, they said.

Following news of the breach last week, Snapchat was quick to respond, noting that its servers were never compromised and that users were instead victimized by their use of third-party apps. Snapchat has warned about the perils of using non-official apps to interact with its service for quite some time.

Those in possession of the images claimed they were trying to organize the trove photos definitely not safe for work, and likely containing pictures of underage Snapchat users into a searchable database. But the creators of Snapsaved.com suggested that’s not likely to happen.

"The recent rumors about the snappening are a hoax," they said. "The hacker does not have sufficient information to live up to his claims of creating a searchable database.

The creators went on to apologize for the breach, and assure users that they have "always tried to fight child pornography," even going so far as to report some of its users to Swedish and Norwegian authorities.

"We never wished for this to happen," the Facebook post reads. "We did not wish to cause Snapchat or their users any harm, we only wished to provide a unique service."

The whole point of Snapchat is to send images that will eventually disappear, but services like SnapSaved are intended to let you save those photos.

Keep Poodle at Bay with Basic Internet Safety

Researchers have uncovered another serious vulnerability in Secure Sockets Layer (SSL) which affects how our information and communications are secured online. The good news is you can take specific steps to block attacks exploiting this flaw.

Google researchers Bodo Möller, Thai Duong and Krzysztof Kotowicz outlined the details of Padding Oracle On Downgraded Legacy Encryption (POODLE) attack in a security advisory posted on OpenSSL.org. The vulnerability is in SSL 3.0, which was introduced in 1996, and replaced by Transport Layer Security (TLS) in 1999. Poodle takes advantage of the fact that clients Web browsers included will downgrade to the older, less secure, protocols if it is unable to establish a secure connection. The downgrade can be triggered by network glitches as well as active attackers.

"Because a network attacker can cause connection failures, they can trigger the use of SSL 3.0 and then exploit this issue," Möller wrote on the Google Online Security Team blog Tuesday afternoon.

Poodle exposes session cookies. The attackers won’t get the user’s password to email accounts or other online services, but will still be able to log in as the user so long as the session cookie is valid. "Thus, while you are at Starbucks, some hacker next to you will be able to post

tweets in your Twitter account and read all your Gmail messages," said Errata Security's Robert Graham.

First Line of Defense?The Poodle attack relies on the adversary first setting up a man-in-the-middle attack to grab control of the victim's Internet connection. One way to do that is to set up a malicious Wi-Fi access point in a public location such as a coffeeshop. Attackers also need to be able to run Javascript code inside the victim's browser.

"It [Poodle] requires someone to be a man-in-the-middle to exploit. This means you are probably safe from hackers at home, though not safe from the NSA.

However, when at the local Starbucks or other unencrypted Wi-Fi, you are in grave danger from this hack," Graham wrote.

So there already are a few things you can do to prevent potential Poodle attacks from succeeding. As we've said time and time again, don't hop willy-nilly on to public Wi-Fi networks or guest networks operated by people you don't know. Even if you aren't worried about Poodle, man-in-the-middle attacks are serious and you protect yourself by being careful about what networks you connect to.

If you need to get on a public network, use VPN, whether from your workplace or any of the many VPN services available. There are quite a few out there, such as PrivateInternetAccess, CyberGhostVPN, and AnchorFree's HotSpot Shield, to name a few.

Attackers will likely trick users into visiting a malicious Web page designed to execute specially crafted Javascript code. Be careful about what sites you visit and be on the lookout for phishing sites.

Why Do We Still Have SSL 3.0??Most modern servers and applications use TLS 1.1 or 1.2, but SSL 3.0 is still widely used in order to support legacy applications and systems. Internet Explorer 6 is one good example. While IE 6 is not as visible as it used to be, it hung around for quite a long time, so quite a number of servers and applications were built to support SSL 3.0 along with the more secure TLS. Netcraft estimated nearly 97 percent of SSL Web servers are likely to be vulnerable.

"You could pretty much kill it in most places today," security researcher Troy Hunt wrote, but that is only part of the problem as there are clients out there which may depend on the ability to fall back to SSL 3.0. We don't know which ones they are, making companies less willing to just pull the plug. For example, there were Twitter reports that MetroTwit, a popular Twitter client for Windows, relied on SSL 3.0 and stopped working after Twitter disabled SSL 3.0 support Tuesday evening (MetroTwit has released a hotfix, by the way, so you should update your client).

"It's the uncertainty that keeps these early generation technologies alive," said Hunt.

Fix the Browser Problem?Use a modern, standards compliant Web browser. Mozilla will disable SSL 3.0 by default in the next version of Firefox, expected Nov. 25, and Google is scrubbing it from Chrome. Safari auto-enables SSL, but Apple has yet to weigh in on its plans for the browser. Microsoft posted an advisory with instructions on disabling SSL 3.0 from Windows desktops and servers.

"No need to hate on Microsoft, as Internet Explorer 10 or 11 will do," said Garve Hays, a solutions architect with NetIQ.

You can manually turn off SSL 3.0 in IE by un-checking the SSL 3.0 box under the Advanced tabs in the Internet Options menu. Firefox users should go to about.config on the browser, and change the value for security.tls.version.min to 1. They can also download a Mozilla add-on to disable SSL 3.0. Chrome users who want to disable SSL 3.0 can add the command line flag --ssl-version-min=tls1 to the browser.

Safari users will have to wait for an update, whenever it comes. Staying off Safari temporarily will reduce the likelihood of a Poodle attack.

When Microsoft stopped supporting Windows XP back in April, there were still holdouts who claimed they didn't see a reason for upgrading to the operating system. If those users are still using Internet Explorer 6, they are going to start seeing things break online. CloudFlare has disabled SSL 3.0 by default for all the sites it hosts, including the 2 million sites which use the free plan. This decision will impact less than 1 percent of all traffic to its sites, Cloudflare said. Many companies are likely to follow Twitter's example and turn off support on their sites. If you still use IE 6 or Windows XP, you really need to upgrade.

"If you're running IE 6 today (yes, there are still some) and you don't have a choice in upgrading because 'reasons', you're stuffed," Hunt wrote.

Facebook Automates Fight Against Hackers

Here's a sneak peek into the system Facebook uses to secure your account when other websites are hacked.

When a hacker reportedly stole 7 million Dropbox user credentials this week, Facebook ensured that the leaked data didn't compromise your Facebook account. Today, the social network offered a peek into the system it uses to keep users' accounts secure, even when other websites are breached.

"Theft of personal data like email addresses and passwords can have larger consequences because people often use the same password on multiple websites," said Chris Long, security engineer at Facebook. "Lots of household company names have experienced the unpleasant phenomenon of seeing account data for their sites show up in these public ['paste'] lists, and responding to these situations is time-consuming and challenging."

Facebook's automated system scans for large-scale data breaches and monitors a selection of sites that hackers commonly use to divulge the stolen data. "Once we find a set of stolen credentials, we pass the data into a program that parses it into a standardized format," Long said.

After Facebook's system downloads and parses the data, it hashes each password using its own internal algorithm. Hashing turns a plain-text password into a string of characters that are nearly impossible to decipher.

Because Facebook stores passwords as hashes, the company can’t compare a password directly to the hacker’s database. "We need to hash it first and compare the hashes," Long explained.

Facebook then uses an automated system to compare each password against its own database of email addresses and passwords for matches. If the hacked credentials match up to your Facebook credentials, the company will guide you through a process to change your password the next time you log in.

If the email and hash combination doesn’t match, it means the stolen password is different from your Facebook password, so hackers won’t be able to use that information to access your account.

"The problem of password reuse on multiple websites is endemic and well documented," Long said. "The risks are also clear: If you use the same password on lots of websites, an attacker only has to get your password once to be able to access all of those accounts."

While Facebook’s process aims to keep your account secure, there are other steps you can take to improve your safety.

Facebook’s Login Approvals option uses two-factor authentication to verify your access from a browser you haven’t used before. To enable this, visit your Security Settings page, check the box next to the Login Approvals option, and click Save Changes.

Your Security Settings page has other options you can opt into to keep your account safe. These include alerts via email, text, message, and push notification if your account is accessed from a computer or device you haven’t used before; adding friends to your Trusted Contacts list, which Facebook will notify if you’ve been locked out of your account; and details such as the browsers you often use and locations where you’ve logged into Facebook, which you can review and revoke access when necessary.

Just when conventional wisdom had converged around the cloud being a software story, there are signs that the server market is poised for an upset, too.

FBI Director Warns That Smartphone Encryption Will Come with Consequences

FBI Director James Comey warned in stark terms Thursday against the push by technology companies to encrypt smartphone data and operating systems, arguing that murder cases could be stalled, suspects could walk free, and justice could be thwarted by a locked phone or an encrypted hard drive.

Privacy advocates and technology experts called the concerns exaggerated and little more than recycled arguments the government has raised against encryption since the early 1990s.

Likening encrypted data to a safe that cannot be cracked or a closet door that won t open, Comey said the move by tech companies to protect user communications in the name of privacy is certain to impede a wide range of criminal investigations. New legislation to allow law enforcement to

intercept communications is needed at a time of advancing technology and new forms of communication, he said.

We have the legal authority to intercept and access communications from information pursuant to court order, but we often lack the technical ability to do so, Comey said in a Brookings Institution speech.

Comey cited particular cases in which he said access to cellphone data aided in a criminal investigation. But in a question-and-answer session after the speech, he said he could not cite particular instances in which someone was rescued from danger who wouldn t have been had law enforcement been blocked from that information.

Rescuing someone before they re harmed? Someone in the trunk of a car or something? Comey asked. I don t think I know yet.

But, he added, Logic tells me there are going to be cases just like that.

The speech, which echoes concerns he and others in law enforcement have previously made, comes soon after announcements by Apple and Google that their new operating systems will be encrypted, or protected with coding by default. Law enforcement officials could still intercept conversations but might not be able to access call data, contacts, photos, and email stored on the phone.

While the companies actions are understandable, Comey said, the place they are leading us is one we shouldn t go to without careful thought and debate.

Encryption isn t just a technical feature. It s a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at every level, Comey said.

The government s concerns may also center in part on the use of Apple s iMessage platform, which offers end-to-end encrypted text messages that supersede traditional SMS messages. That kind of encryption likely provides access to those messages on users iPhones, of which Apple has sold more than 240 million since 2013.

He acknowledged a rise in public mistrust of government in the year since former National Security Agency systems analyst Edward Snowden revealed NSA secret intelligence collection programs. But he said the public was wrong to believe that law enforcement can access any and all communications with the flip of a switch.

It may be true in the movies or on TV. It is simply not the case in real life, he said.

Comey also said the FBI was committed to a front-door approach, through court orders and under strict oversight, to intercepting communications. Privacy advocates have long been concerned that that development would create an opening for hackers to exploit. The American Civil Liberties Union noted that federal law protects the right of companies to add encryption with no backdoors and said the companies should be credited for being unwilling to weaken security for everyone.

Whether you call it a front door or a back door, weakening the security of a system to enable law enforcement access also opens that door to foreign governments and criminals, said Christopher Soghoian,

principal technologist with the ACLU s Speech, Privacy, and Technology Project.

Matthew Green, a cryptology professor at Johns Hopkins University, said the debate over personal encryption isn t new: Back in the 1990s, when personal computers were a novelty, he said most consumers weren t even aware of encryption. When a form of email encryption called PGP was released, he said, there was a fear that criminals would use it.

These technologies exist for consumers to protect their privacy, he said, and it s very hard to do anything about it.

The Center for Democracy and Technology said in a statement that law enforcement already has ways to obtain the electronic data it needs.

Encryption of our personal devices and communications enhances the security of our most private information, the center said.

NSA Reviewing Official’s Part-time Private Work

The National Security Agency is reviewing its decision to allow a top official to work part time for a cybersecurity firm that is pitching its services to the financial sector, the agency said on Friday.

NSA’s chief technical officer, Patrick Dowd, was given permission to work up to 20 hours a week at IronNet Cybersecurity, a private firm. The company was founded by Keith Alexander, a retired Army general who used to run the NSA and the U.S. Cyber Command.

The arrangement raises a host of questions, because the NSA has access to classified information about cyberthreats. IronNet expects to make "a lot" charging companies to protect them from such threats, Alexander told The Associated Press in August.

NSA said in a statement on Friday that the situation "is under internal review. While NSA does not comment on specific employees, NSA takes seriously ethics laws and regulations at all levels of the organization."

Alexander and Dowd_whose other title at NSA is "chief architect"_did not immediately respond to requests for comment on Friday.

This isn’t the first time IronNet has raised eyebrows. When Alexander founded the company after he retired in March, he disclosed that the firm was developing as many as 10 patents for a new model of cybersecurity. There were reports that he was charging financial sector firms $1 million a month. He said that figure was high, but he declined to disclose the firm’s fees.

Critics questioned Alexander’s contention that he was not seeking to profit from his years of experience battling cyberthreats in the secret world of the NSA and cyber command.

Alexander spent nine years as NSA director, ended his career dealing with the stunning revelations of former NSA systems analyst Edward Snowden.

How The ’Safest Place on The Internet’ Tracks Its Users

In an elegant warehouse-style building on Venice Beach known locally as the fortress , Michael Heyward, a tech entrepreneur, was struggling to control the remote-controlled drone hovering above the heads of his employees.

The 27-year-old son of Andy Heyward, one of cartoon character Inspector Gadget s co-creators, giggled as the drone came crashing down to the floor, narrowly missing the head of a female developer.

Outside the building, once owned by Hollywood royalty Anjelica Huston, skateboarders, surfers, tourists and the homeless mingled in the Californian sun. It was just another day on Silicon Beach a name the local tech crowd loathe, but one that has come to define a new generation of savvy, young firms sprouting up in Los Angeles, challenging the tech giants of San Francisco.

One of the hottest new kids on the block is Whisper, the company Heyward co-founded, which is part of a new wave of Venice Beach-based social media companies that have grown up in Facebook s shadow. Snapchat is next door; Tinder, the dating app, is round the corner.

Whisper s selling point is anonymity. It describes itself in the app store as the first completely anonymous social network .

For Heyward the established social media networks Facebook and Twitter have created a dilemma. People can no longer speak honestly; they self-censor for fear of being judged by their peers, colleagues and family, or portray only idealised version of their lives.

Whisper is a platform for the truth, however ugly.

A quick look at the app proves the point. I push great guys away because I m terrified they will leave like my dad did. I hate him for causing this, reads one message you would be unlikely to see on Facebook. That moment when ur mum tells u she hates u because ur gay 17/M/gay, reads another.

Hate speech, real names, pornography, drug dealing and other offences are all sifted out of the app. Some 40,000 people mentioning suicidal tendencies have been automatically referred to a suicide hotline. Whisper has set up a nonprofit, Your Voice, to help raise awareness of mental health issues.

Whisper now hosts more than 2.5m messages every day, an outpouring of intimate confessions made on a platform Heyward has described as the safest place on the internet .

But Whisper has a secret.

The Guardian was given access to the company s back-end system the tool they use to sift through the millions of messages posted via the app each week and spoke at length with the company s staff to explore the possibility of an expanded partnership.

Whisper s internal practices appeared at odds with Heyward s public declarations, some of the company s terms of service and, in all probability, the expectations of users who are downloading the app in

growing numbers on the assumption it will give them a cloak of invisibility.

The company denies this, pointing to its policy of not collecting information such as user names, phone numbers or addresses that would easily identify them. Whisper does not collect nor store any personal identifiable information from users therefore their privacy and anonymity are always protected, the company said in a statement.

But four days after Whisper learned the Guardian planned to make public its internal practices, the company quietly rewrote its terms of service and introduced a new privacy policy.

Furnished with an extremely simple password, we were given access to the company s vast library of texts and photographs and, in most cases, the location of their authors. The company s developers have created a back-end analytics tool to conduct more refined searches of the database, the most powerful of which pinpoints location.

Whisper s in-house mapping tool identifies users who have posted from GuantÆnamo Bay, Cuba, using their GPS data. Occasionally, the company uses IP address location data to establish the rough location of some users who have opted out the app s geolocation services.

The location information is salted accurate to within a 500-metre radius of a phone, Whisper says and staff work on the basis that they can identify a user s street, or neighbourhood, but not usually their home unless they live in a rural area.

But that still allows Whisper to use its mapping tool to trawl for all the users in one place.

There were postings from GuantÆnamo Bay, Cuba, the US naval facility on Diego Garcia, in the Indian Ocean, the National Security Agency in Maryland and the CIA at Langley, Virginia.

Many of the messages were banal expressions of boredom, or solicitations for sex; some hinted, however vaguely, at potential abuses of power.

On top of a picture of a whip, a user who appeared to be inside the Pentagon posted: I love being a sadist and breaking women. A user inside Nevada s Creech air force base, the remote military compound where US military drones are controlled, posted the phrase Allah Ahkbar over a picture of a grenade.

There were 12 Whispers seemingly posted from within of grounds of the White House. One message, superimposed over a picture of President Barack Obama, said: I m so glad this app is anonymous. The press would have a field day if they knew some of the stuff I post on here.

A Whisper user posted this message from the vicinity of the White House. The red dots indicate Whisper messages sent from that location. Potentially identifying information has been redacted by the Guardian.

Of course, just because the user posted from inside the White House, does not mean they work in the West Wing. They could be secret service agent, a cleaner, a journalist or one of the hundreds of visitors given temporary access to the presidential residence each week.

But while Whisper stresses it does not collect information that

immediately identifies a user, geographical information, stored over time, leaves a digital footprint of clues to a person s true identity.

To the public, Whisper postings are disconnected from each other. Users do not have a history of messages that can be looked up and inspected by other users.

But Whisper s in-house tools do offer that power of investigation. The company s staff are trawling through past messages even those the user believes they have deleted inspecting the precise date, time and approximate location of each message.

Whisper insisted in its statement to the Guardian that it does not follow or track users .

The location of users who have turned off Whisper s geolocation service is not automatically uploaded onto the company s mapping tool. However the rough location of those users is retrieved, on demand, for a news unit headed by the company s editor-in-chief, Neetzan Zimmerman.

The company stressed in the statement that this data, based on a phone s IP address, is a very coarse and unreliable source of location information .

Whisper s interest in delving into the prior movements of users is rooted in the company s emerging business model. Striving to build awareness for an app that s in fierce competition with rivals Secret, Yik Yak and now another proposed anonymous message service from Facebook, it is curating and promoting interesting content.

Whisper hired Zimmerman, a former editor at Gawker who specialised in viral content, to lead a concerted push to promote the messages appearing on its app. The company does not see itself as a news organisation as such, but Zimmerman is tasked with turning some of the juiciest confessions appearing on the app into page views and publicity.

But there is a problem. If users are anonymous, how can Whisper know if they are telling the truth?

Hence, the company s desire to dig into the background of certain users. Location, Whisper has discovered, gives a strong hint of who a user might actually be.

If a user claims to be in the US marines, for example, Whisper will track their movements to see if they ve spent time on a military base. If a user claims to be a college student, Whisper will track their whereabouts to see if they are based on a college campus.

Those who have opted into geolocation services are easiest to track. For the estimated 20% of users who have opted out of geolocation services, Whisper turns instead to their IP data. These constitute a sizeable portion of users being targeted for special attention by Whisper.

In a widely read Buzzfeed article drawing on 23 Whisper postings about assault in the military, for example, five came from people who had disabled their geolocation services. The article said Whisper had vetted every account using our back-end tools and filtered out any we thought might be bogus claims but did not specify how that was done.

The five users who had explicitly opted out of geolocation services, but

were featured in the article anyway, included one who said she was gang raped after having an abortion in the army, and another who said they had been were drugged and raped by two marines.

Whisper said in its statement: Whisper does not request or store any personally identifiable information from users, therefore there is never a breach of anonymity. From time to time, when a user makes a claim of a newsworthy nature, we review the user s past activity to help determine veracity.

On Thursday, a Buzzfeed spokesperson said the news outlet is now halting its partnership with Whisper. We re taking a break from our partnership until Whisper clarifies to us and its users the policy on user location and privacy, the spokesperson said.

Zimmerman acknowledges there are complex ethical issues that the tech start-up is still grappling with internally. Like Heyward, he can sound almost evangelical about Whisper s potential to fulfill a public good.

Both see the company as a potentially trusted haven for whistleblowers, a safe place for people to air their most private thoughts.

But a look behind the curtain at Whisper raises difficult questions about the burden of responsibility the company acknowledges it is shouldering.

 Anonymity is a very powerful tool, Heyward told a Bloomberg reporter in March. There s a Spider-Man quote that says with great power comes great responsibility. It is a famous one. We view anonymity very much in the same way.

New Wild West of Domain Names Includes Everything from .beer to .bmw

Heather Parker is a technically savvy businesswoman. She has her own Heather Parker Photography website, she knows about social media and search-engine optimization; she publishes examples of her work on Yelp.

But she didn t know about one of the biggest changes happening right now: a massive expansion of Internet address domains beyond the well-known .com, .net, and .org. If she wanted, she could move her website to heatherparker.photography today.

 I didn t know .photography was something I could register for until now, Parker said. She s not going to, because clients likely wouldn t know what it meant if they saw it on a business card, she added.

That lack of awareness is one challenge facing domain-name expansion and the nonprofit organization behind it, the International Corporation for Assigned Names and Numbers, or ICANN. Another is a rat s nest of global trademark complications as companies try to protect their brands on hundreds of new Internet domains.

One example: Two Merck pharmaceutical companies, one with rights to use the name in the U.S. and Canada and the other with rights in the rest of the world, are fighting in court over the .merck domain. Another: A UK company called Yoyo.email has registered hundreds of .email subdomains with others trademarks, including dunkindonuts.email, budlight.email, sheraton.email, lufthansa.email, eharmony.email, footlocker.email and

ebaysupport.email.

But the new domain names are here to stay, and businesses and consumers must adjust to the new reality. ICANN approved hundreds of the 1,930 applications for the new domains, with 417 on the Internet already.

The .com suffix had special meaning for the first generation of Internet users. For children born this century, it ll be just one fish in the sea.

And there will be plenty more fish coming. Another round of applications likely will open up by 2018, said Akram Atallah, president of ICANN s global domains division. That next round will be one subject of discussion at an ICANN meeting this week in Los Angeles along with what ICANN should do with the millions of dollars it s garnered so far from the program.

More fish? What are some of the other domains? There are brand names like .ibm, .youtube, .axa, and .bmw. There are geographic names like .paris, .budapest, and .berlin. There are business terms like .realtor, .beer, .dentist, .pizza, and .plumbing. There are broad terms like .xyz, .pink, .email, .work, and .website. And there are many that take advantage of ICANN s expansion beyond the Latin character set.

As ever, when there s change on the Internet, there s someone there to profit from it. Perhaps the highest-profile is a startup called Donuts, backed by more than $100 million from investors to run a new business doling out subdomains to businesses in dozens of categories. It ll take some time to educate the market, said Dan Schindler, the company s co-founder and executive vice president of sales and marketing, but eventually businesses will see the new domains simply as a way to instantly signal to customers what they do.

 We view these as better than .com, which is meaningless. They re short, specific, and meaningful, Schindler said. The numerous brands embracing the new domains will teach people about the new era, he added. When you see 3series.bmw and 5series.bmw appear on TV screens and billboards around the world, it ll drive awareness [a website] doesn t have to end in .com.

People have registered more than a million addresses that use Donuts top-level domains, the company said Monday, with the millionth being heavenly.coffee. That s a small fraction of the 1.03 billion website in existence, according to monitoring firm Netcraft, but new domains have been available for just under 12 months.

ICANN expanded the domain-name pool to provide more choice, competition, and innovation, Atallah said. The choice and competition is visible today, but the innovation will become more visible when big brands like Apple jump aboard.

 If you re applying for .apple, the way you use it should be innovative. It s defining how you present yourself online, he said, and it comes with an authenticity factor that guarantees to customers that they re at the the right place.

How do domains work? In the Internet s earliest years, addresses ended with one of seven three-letter abbreviations: .net, .gov, .edu, .mil, .int, .org, and .com. These suffixes are called top-level domains. To be useful, they need to be accompanied by a subdomain before the dot: stanford.edu, redcross.org.

The initial set of top-level domains was joined by country-code domains like .jp for Japan and .za for South Africa. But often the prime virtual real estate ending in .com was taken, and ICANN tried to expand the system with what are now called generic top-level domains (GTLDs).

According to figures from GreenSec Solutions NTLDstats site, .xyz is the most used of the new top-level domains.

ICANN oversees the master list, but many others are involved. Organizations called registries oversee the supply of subdomains for each domain; for example, Verisign operates the .com registry. Next down the hierarchy are organizations called registrars that actually register the domain names on behalf of the people who want to use them.

Here s an example of how it works. If Main Street Florist wants to set up business online, they can pay a registrar like GoDaddy to register mainstreet.florist, with prices sometimes less than $20 per year but sometimes more than $100 annually. A portion of that registration fee flows back to the registry in this case, Donuts, which operates the .florist registry.

Registries pay ICANN for the privilege. Each of the 1,930 new applications to operate one of the new GTLD registries came with a $185,000 application fee, and running the registry costs $25,000 a year on top of that. Atallah said he expects fees to go down when ICANN opens the second round of GTLD applications later this decade.

In this round, costs can go and have gone higher, too: when more than one party wants to operate the same registry, ICANN holds an auction and awards rights to the highest bidder. Right now, 402 domains are under contention with multiple applicants, with the highest demand going for the .app registry. Some of this string contention is resolved through private auctions, too, in which case ICANN doesn t get any extra proceeds from the auction.

String contention can be expensive. Amazon outbid Google, among others, paying $4.6 million for .buy. And a company called Dot Tech acquired rights to .tech for $6.8 million.

 The purpose of .tech is to provide a dedicated online environment for the technology industry, allowing businesses to create user-friendly access to products, services and information instantaneously through accurate search engine classifications, the company said in its application. It hopes businesses using .tech will become differentiated online as tech-savvy innovators, product suppliers or service professionals.

Trademark hurdles? Dot Tech is excited, but established brands castigated ICANN s domain-name expansion plans because of new trademark hassles. Companies are accustomed to buying rights to their name on the .com registry, and maybe a handful of others like .info, .co, and .biz. With hundreds and later thousands of new domains, that s simply not practical anymore, and that raises the possibility that cybersquatters will register a company s name on a new domain. They can set a webpage festooned with ads on it or redirect traffic to a different site of their choosing. And of course they can profit when the trademark holder buys the rights to the site.

The domain-name expansion is an opportunity for brands but it s big

opportunity for cybersquatters. You re seeing it time and again, said David Taylor, a lawyer at Hogan Lovells International who specializes in domain-name issues. Brands will be put to a higher cost.

Taylor was a member of a group of experts ICANN convened to try to ease trademark issues. ICANN adopted several of its recommendations. That includes the Uniform Rapid Suspension (URS) System that s designed to be cheaper and faster than the earlier Uniform Domain-Name Dispute-Resolution Policy (UDRP) when brand holders want to contest another party s domain-name registration; a sunrise period that lets trademark holders be the first to register their own trademarks on new domains; and the Trademark Clearinghouse that gives trademark holders a central place to register their marks for domain-related purposes.

For $150 a year, the clearinghouse will notify trademark holders of domains involving their trademarks and validate their trademarks if they re registering them during a new domain s sunrise period. As of Sept. 16, trademark holders registered 32,993 trademarks, and the clearinghouse sent out 111,855 notices of domain-name actions involving those trademarks.

Trademark holders need to be aware of the repercussions of the new domain names, said Peter Van De Wielle, the Trademark Clearinghouse s marketing manager. That s why we re focusing resources on education, he said.

Yoyo.email case? The Yoyo.email case indicates how complicated things can get. The company has been involved with at least 34 URS and UDRP cases involving domain names it s registered that involve others trademarks. Yoyo.email founder Giovanni Laporta said in correpondence with CNET that he s no cybersquatter   indeed, that he didn t even know what a cybersquatter was until trademark lawyers came after his business. And he s now fighting some of those cases in court. Here s how he described his business:

 Yoyo plans to launch a new email hosting platform, which amongst many other innovative features [has] a certified email service. Yoyo can only guarantee the service if it controls both ends of the email send and receive process. The brand.emails are only used to internally route emails so that all the metadata is captured on our servers. That way Yoyo can certify that the email was sent and, in some instances, received. Like certified mail, there has to be proof that someone sent a person to someone s door and put in in the box. The brand.email is just an easy way to route and store the data, invisible to sender and receiver.

Yoyo won t involve websites using the domains, and indeed Laporta refused an offer to sell the StuartWeitzman.email domain to shoe and purse seller Stuart Weitzman for $1,000. Selling any of our <.email> domains will be detrimental to service operation. Selling domain names is not the reason why domain names were registered, so I respectfully have to decline your offer, he said in a letter to the company s attorney.

Regardless of Yoyo s intentions, brand holders have been leery of new domains for years. A presence on the Internet has been an exciting new way to interact directly with customers, but each new service   email, the Web, Facebook, Twitter, Google+, Pinterest, ad networks, app stores, and more   means another area where they have to worry about their reputation. The value of that brand can be immense. Last week, Apple topped Interbrand s annual survey of brand value, worth an estimated $119 billion.

More fees? In addition to ICANN s official mechanisms for dealing with trademark worries, companies can pay for more protection. For about $3,000, Donuts will block registrations for five years of particular names across its own registries but not others registries.

Another startup, BrandShield, scours new Net domains and other online areas for trademark problems and then ranks them for clients. It costs $1,000 a year for small companies but goes up for those with a bigger online presence.

 Our algorithms automatically prioritize the level of risk to give you a rank so you can focus on the ones that really create damage, said Yoav Keren, chief executive of BrandShield.

For her part, photographer Parker isn t racing either to embrace the new domains or to mount new defenses.

 I know people will squat on these new domain names and there will be speculation. I m not too worried about it, she said. If it ain t, broke don t fix it.

In the long run, ICANN expects the pain and uncertainty will be worth it especially for companies that set up their own branded domains.

 When you are in a general space, everything goes. When you are in a specific space, you can present yourself differently, Atallah said. You have the ability to control your destiny.

How To Prepare Your Mac for the OS X Yosemite Upgrade

Mac OS X 10.10 Yosemite is out, but there are four things you need to do before upgrading your Mac to Apple s latest operating system.

1. Check if your Mac is able to run Yosemite.?According to Apple, the following are the supported models for Yosemite:

iMac (mid 2007 or newer)
MacBook (late 2008 Aluminum, or early 2009 or newer)
MacBook Pro (mid/late 2007 or newer)
MacBook Air (late 2008 or newer)
Mac mini (early 2009 or newer)
Mac Pro (early 2008 or newer)
Xserve (early 2009)

If you can t remember your Mac s vintage, click the Apple logo in the upper-left corner and choose About This Mac. A small window will pop up, showing basic system information.

To see what year your Mac was made, click the More Info button, and you ll see a bit more system information, including your Mac s era in gray lettering below its name.

2. Make sure you have enough memory and hard drive space.

Among Yosemite s general requirements are a minimum of 2 GB of memory and at least 8 GB of available space. The memory amount is shown on the main

About This Mac screen from above. To see how much space you have on your Mac s hard drive or SSD, click the More Info button again and then click Storage at the top of the window.

3. Check your current OS X version.?If you haven t updated your Mac s operating system in a number of years, then you need to check to see if you are running at least OS X 10.6.8 Snow Leopard, which was released way back in 2009. Its 10.6.6 update introduced the Mac App Store, which you ll need to download Yosemite. The About This Mac window will show which version of OS X you have. You need be running one of the following:

OS X Snow Leopard (10.6.8)
OS X Lion (10.7)
OS X Mountain Lion (10.8)
OS X Mavericks (10.9)

If you have an ancient Mac whose OS predates Snow Leopard, you will need to install Snow Leopard before then moving to Yosemite. You can buy Snow Leopard for $19.99 here.

4. Before you do anything, back up your Mac. If you have determined that your Mac can run Yosemite, then your first move before upgrading is always to perform a system backup to protect your data. Should the installation go awry, you don t want to lose important documents along with your photo and music libraries. Thankfully, Macs include a tool that make backups easy: Time Machine.

10 Ways To Protect Your Home Network from Hackers

Protecting your family s digital assets used to be easy. You just turned on your PC s built-in firewall settings and turned on an antivirus program. As long as you didn t install strange software or do anything stupid, you were usually OK.

Times have changed. Now you can get infected just by visiting a compromised website. Organized gangs of cybercriminals are trying to break into your bank account, steal your identity, or take control of your home network to send spam and launch attacks against other machines.

And instead of just one machine to protect, you might have a dozen including mobile phones, game consoles, streaming video boxes, and smart appliances all vulnerable to attack. Just like a big, juicy corporate network. In fact, as big companies make their networks harder to break into, cybercrooks are moving to home networks, says Michael Kaiser, executive director of the National Cyber Security Alliance.

Every family needs its own chief security officer, someone who spends time thinking about all the digital components in their lives and what they re doing to secure them, says Kaiser, whose organization operates the Stay Safe Online Web portal and sponsors National Cyber Security Awareness Month each October.

Odds are that someone is you. There are several things you can do to persuade the bad guys to move on to easier targets. It starts with the gateway to most of the digital devices in your home: your wireless router.

1. Fortify your WiFi.?Hopefully, by now you ve changed the default log-in name and passwords for your WiFi router and turned on WPA or WPA2 encryption. (If not, do it now I ll wait.) Instructions for each router vary; your best option is to visit the manufacturer s support site to find out how.

You also need to make sure your router s internal sofware (aka firmware) is up to date. Last February, security researchers Team Cymru discovered a security hole in more than 300,000 routers that could allow a remote attacker to hijack any home network and access all the machines attached to them. Again, the router maker s website should have information on how to update firmware; some will let you set the router to update itself automatically.

If you ve recently bought a new router, register it with the manufacturer, either online or by mailing in the reg card that came in the box, suggests Robert Siciliano, online security expert for McAfee. That way you ll be notified if there are any security updates available.

2. Install antivirus software and keep it up to date. This should be obvious, but according to Microsoft s annual Security Intelligence Report, one out of four PCs in the US is not running up-to-date antivirus software, making them nearly six times more likely to get infected than those that are. The numbers for mobile devices are downright shocking only one in 20 smartphones is protected, says research firm IDC.

Malware scanners won t catch everything, admits Stephen Cobb, senior security researcher for ESET North America, makers of security software for PCs, Macs, and Android devices. But a properly licensed anti-malware program can protect you against the vast majority of online threats, even some zero day threats that have never been seen before, he adds.

At the moment, malware that targets phones and tablets is still somewhat rare. Over the next couple of years, that is guaranteed to change. Fortunately, there are plenty of security apps for your mobile devices, many of them free. Some of the top iPhone security apps are made by Trend Micro, McAfee, and Lookout Mobile. Aside from ESET Mobile Security, you can find highly recommended anti-malware Android apps from Avast and Avira.

3. Update your operating systems early and often. Attackers love crawling through holes in your computer s operating system, which is why you always want to be running the latest version of your OS. Yet, according to security vendor Secunia, nearly 13 percent of operating systems aren t up to date.

The easiest way to keep Windows up to date is to tell it to automatically download and install updates as they appear. This will cause your system to reboot, which could thoroughly bollix any work you haven t saved, although the system will alert you before a reboot. (Security updates are usually distributed every second or fourth Tuesday, so you can also plan ahead.) In OS X, you ll want to go into System Preferences, launch the App Store app, and make sure it s set to automatically install security updates.

4. Patch your software till it hurts. You know those seemingly constant reminders to update various bits of software? Odds are it s because there s a security hole that needs to be plugged. According to Secunia, one in nine software programs is left unpatched. And two of the least

frequently updated programs Oracle Java and Adobe Reader are also among the most vulnerable to attack.

Yes, updating software is a total pain. Fortunately for Windows owners, Secunia s free Personal Software Inspector (PSI) can scan all your software, automatically locate any necessary updates, and install them automatically. The bad news? You ll have to scan each computer on your network separately, and there are no consumer-friendly auto-patch options for Macs.

5. Ditch outdated applications.?Once software has reached the end of its commercial life and the publisher has stopped supporting it, it s really time to move on. (I m talking to you, the 24 percent of people who still run Windows XP.) Why? Because if some enterprising hacker finds a new security hole, there will be no patch to add. You re a sitting duck for any new exploit.

6. Get real about passwords.?Until something better comes along, we are still mostly stuck using passwords to protect our most sensitive devices and accounts. Hopefully you ve read enough stories about people s accounts being hacked because they used password as a password to choose a more complicated one the longer, the better. Or use an encrypted password manager like 1Password, Dashlane, LastPass, or MaskMe to generate complicated passwords and remember them for you. Don t make me come over there.

7. Turn on two-factor authentication. Even complex passwords can be cracked with enough effort, Siciliano notes.

 A determined hacker can use a plain ol laptop to crack long passwords, he says. Tools to do the dirty work are available for free or just a few bucks.

Adding a second factor like a PIN code sent via SMS that you have to enter into a form along with your password helps cut down on a stranger s ability to access your account. If someone attempts to access your account from an unknown device, you ll receive an alert, giving you an opportunity to go in and change your password before the bad guys get your stuff.

8. Wipe your old hardware. Old hard drives, USB sticks, phones, and backup discs can be chock-full of highly personal data as well as passwords and other log-on credentials. Make sure to wipe them clean before you resell them. Or physically destroy them before you recycle.

9. Shut up on social media. You don t have to go dark on Facebook or bury your Twitter account. But you don t need to share every facet of your life with total strangers, either. Avoid exposing personal information that could also be the answer to password reset security questions (your mom s maiden name, your first pet, your high school, and so on).

This kind of information helped hackers break into the iCloud accounts of Jennifer Lawrence, Rihanna, and other celebutantes. Don t let it happen to you or your kids.

10. Rally the troops. ?Remember how I said that in an earlier, more innocent time, you were usually OK as long as you didn t do anything stupid? That advice still applies, but the definition of stupid has expanded to clicking on unexpected mail attachments, falling for phishing emails, visiting dodgy websites, and oversharing on social

media.

You ll need to call regular family meetings to make sure everyone understands the risks and is playing by the same rules, Kaiser says.

No bones about it playing family chief security officer is a crappy job. But if you don t do it, you not only put your family s finances and information at risk, but you also make the Internet a little less safe for everyone. Cybersecurity really does start at home.

=~=~=~=